CLAIMS:

1. A method, comprising:

converting original data into a plurality of sub-bands using wavelet decomposition;

encrypting at least one of the sub-bands using a key to produce encrypted sub-band data; and

transmitting the encrypted sub-band data to a recipient separately from the other sub-bands.

2. The method of claim 1, further comprising embedding at least one message in the at least one sub-band prior to the encryption step.

3. The method of claim 2, wherein the at least one message is at least one of hashed, digitally signed for, and encrypted prior to embedding the at least one message in the at least one sub-band.

4. The method of claim 3, wherein a private key is employed when the at least one message is digitally signed for, and a secret key is employed when the at least one message is encrypted.

5. The method of claim 1, wherein the at least one message is a digital signature, which is transmitted to the recipient to verify the integrity of the encrypted sub-band data.

6. The method of claim 1, further comprising:

encrypting a plurality of the sub-bands using respective secret keys to produce respective encrypted sub-band data, each secret key being the same or different from one of more of the respective secret keys; and

transmitting the respective encrypted sub-band data over at least some differing routes of a packet-switched network to the recipient.

7. A method, comprising:

permitting a source entity to make a protocol selection concerning (i) parameters of a wavelet decomposition process to which original data are to be subject to convert the original data into a plurality of sub-bands, and (ii) parameters of an encryption process to which at least one of the sub-bands is to be subject to produce respective encrypted sub-band data; and

permitting the source entity to select a respective security level to be associated with the respective encrypted sub-band data;

comparing at least one of the protocol selection and selected security level(s) with a database containing data concerning at least one of (i) a probability that the encrypted sub-band data may be broken given the protocol selection, (ii) an association between security levels and protocol selections; and

advising the source entity to select at least one of a different security level and a different protocol when a result of the comparison indicates a relatively high probability that the encrypted sub-band data may be broken.

8. The method of claim 7, wherein the protocol selection further includes at least one of: (i) parameters of a hashing process to which at least one message is to be subject prior to embedding the at least one message in one or more of the sub-bands, (ii) parameters of a digital signature to which the at least one message is to be subject prior to embedding the at least one message in one or more of the sub-bands, (iii) parameters of an encryption process to which the at least one message is to be subject prior to embedding the at least one message in one or more of the sub-bands, and (iv) aspects of nodes of a packet-switched network through which the respective encrypted sub-band data are to traverse for transmission to a recipient.

9. The method of claim 7, further comprising:

converting the original data into a plurality of sub-bands using the selected parameters of the wavelet decomposition process;

encrypting at least one of the sub-bands to produce encrypted sub-band data using the selected parameters of the encryption process; and

transmitting the encrypted sub-band data to the recipient as one or more separate packets from the other sub-bands.

10. The method of claim 9, further comprising:

encrypting a plurality of the sub-bands using respective secret keys to produce respective encrypted sub-band data, each secret key being the same or different from one of more of the respective secret keys; and

transmitting the packet(s) of the respective encrypted sub-band data over at least some differing routes of the packet-switched network to the recipient.

11. The method of claim 9, further comprising routing the packet(s) of the encrypted sub-band data to the recipient over trusted nodes of a packet-switched network, each trusted node having a node security level for comparison with the security level(s) associated with the respective encrypted sub-band data, wherein each packet may only be routed through a trusted node having a node security level equal to or higher than the security level associated with the encrypted sub-band data.

12. The method of claim 11, wherein at least one of:

the node security levels of the trusted nodes are time variant in response to network conditions; and

each node is capable of changing its security level in response to the network conditions.

13. The method of claim 11, further comprising merging two or more packets of the respective encrypted sub-band data into one or more further packets within a trusted node having a security level equal to or higher than the security level associated with the encrypted sub-band data.

14. An apparatus including a processor operating under the instructions of a software program, the software program causing the apparatus to perform actions, comprising:

converting original data into a plurality of sub-bands using wavelet decomposition;

encrypting at least one of the sub-bands using a key to produce encrypted sub-band data; and

transmitting the encrypted sub-band data to a recipient separately from the other sub-bands.

15. The apparatus of claim 14, further comprising embedding at least one message in the at least one sub-band prior to the encryption step.

16. The apparatus of claim 15, wherein the at least one message is at least one of hashed, digitally signed for, and encrypted prior to embedding the at least one message in the at least one sub-band.

17. The apparatus of claim 16, wherein a private key is employed when the at least one message is digitally signed for, and a secret key is employed when the at least one message is encrypted.

18. The apparatus of claim 14, wherein the at least one message is a digital signature, which is transmitted to the recipient to verify the integrity of the encrypted sub-band data.

19. The apparatus of claim 14, further comprising:

encrypting a plurality of the sub-bands using respective secret keys to produce respective encrypted sub-band data, each secret key being the same or different from one of more of the respective secret keys; and

transmitting the respective encrypted sub-band data over at least some differing routes of a packet-switched network to the recipient.

20. An apparatus including a processor operating under the instructions of a software program, the software program causing the apparatus to perform actions, comprising:

permitting a source entity to make a protocol selection concerning (i) parameters of a wavelet decomposition process to which original data are to be subject to convert the original data into a plurality of sub-bands, and (ii) parameters of an encryption process to which at least one of the sub-bands is to be subject to produce respective encrypted sub-band data; and

permitting the source entity to select a respective security level to be associated with the respective encrypted sub-band data;

comparing at least one of the protocol selection and selected security level(s) with a database containing data concerning at least one of (i) a probability that the encrypted sub-band

data may be broken given the protocol selection, (ii) an association between security levels and protocol selections; and

advising the source entity to select at least one of a different security level and a different protocol when a result of the comparison indicates a relatively high probability that the encrypted sub-band data may be broken.

21. The apparatus of claim 20, wherein the protocol selection further includes at least one of: (i) parameters of a hashing process to which at least one message is to be subject prior to embedding the at least one message in one or more of the sub-bands, (ii) parameters of a digital signature to which the at least one message is to be subject prior to embedding the at least one message in one or more of the sub-bands, (iii) parameters of an encryption process to which the at least one message is to be subject prior to embedding the at least one message in one or more of the sub-bands, and (iv) aspects of nodes of a packet-switched network through which the respective encrypted sub-band data are to traverse for transmission to a recipient.

22. The apparatus of claim 20, further comprising:

converting the original data into a plurality of sub-bands using the selected parameters of the wavelet decomposition process;

encrypting at least one of the sub-bands to produce encrypted sub-band data using the selected parameters of the encryption process; and

transmitting the encrypted sub-band data to the recipient as one or more separate packets from the other sub-bands.

23. The apparatus of claim 22, further comprising:

encrypting a plurality of the sub-bands using respective secret keys to produce respective encrypted sub-band data, each secret key being the same or different from one of more of the respective secret keys; and

transmitting the packet(s) of the respective encrypted sub-band data over at least some differing routes of the packet-switched network to the recipient.

24. A system, comprising:

a source entity operable to: (i) convert original data into a plurality of sub-bands using a wavelet decomposition process, (ii) encrypt at least one of the sub-bands to produce encrypted sub-band data, and (iii) transmit one of more packets of the encrypted sub-band data to a recipient over a packet-switched network separately from the other sub-bands; and

a plurality of trusted nodes within the packet-switched network, each trusted node having a node security level for comparison with a security level associated with the encrypted sub-band data,

wherein each packet may only be routed through a trusted node having a node security level equal to or higher than the security level associated with the encrypted sub-band data.

25. The system of claim 24, wherein at least one of:

the node security levels of the trusted nodes are time variant in response to network conditions; and

each node is capable of changing its security level in response to the network conditions.

26. The system of claim 24, wherein at least some of the trusted nodes are operable to merge two or more packets of the encrypted sub-band data into one or more further packets when the given trusted node has a security level equal to or higher than the security level associated with the encrypted sub-band data.